NORGES BANK

2021

FINANCIAL INFRASTRUCTURE REPORT

Selected key figures

Daily turnover in Norges Bank's settlement system

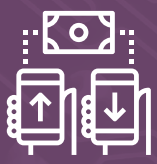
458bn

Daily number of transactions in the Norwegian Interbank Clearing System (NICS)

10m

Daily turnover in securities settlement

104bn



Mobile share of P2P payments

80%

Contactless share of BankAxept payments

80%

Number of banks

122

Daily turnover in Norges Bank's settlement system: Average for 2020. Source: Norges Bank.
Daily number of transactions in the Norwegian Interbank Clearing System (NICS): Average for 2020. Source: Bits.
Daily turnover in securities settlement: Gross turnover. Average for 2020. Source: Euronext VPS.
Mobile share of P2P payments: Survey conducted spring 2021. Source: Norges Bank.
Contactless share of BankAxept payments: Average for April 2021. Source: BankAxept.
Number of banks: Number of banks with an account with Norges Bank. At year-end 2020. Source: Norges Bank.

Financial Infrastructure Report 2021 – in a nutshell

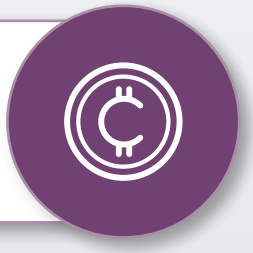
The financial infrastructure has functioned smoothly
There have been few disruptions in the Norwegian financial infrastructure in recent years, and the infrastructure has functioned smoothly also during the coronavirus pandemic. We consider the financial infrastructure to be secure and efficient.

New framework for strengthening cyber resilience
Testing for and identifying risks of cyber incidents in the banking and payment system can be improved. Finanstilsynet (Financial Supervisory Authority of Norway) and Norges Bank have drawn up a proposed framework for testing cyber resilience. The proposal has been circulated for comment this spring.

Real-time payments should be available in more payment situations
The infrastructure for real-time payments has been strengthened, but there is still a need for improvements and further development of retail services atop this infrastructure. Norges Bank is now assessing how the real-time payment infrastructure can best be further developed, including whether Norges Bank should expand its operational role.

Need to clarify the regulation of cash services
For cash to help promote confidence and efficiency in the payment system, cash must be available and easy to use. Norges Bank supports the drafting of a regulation that clarifies the obligation of individual banks to ensure that customers have the opportunity to deposit and withdraw cash. It should also be specified how banks can take into account electronic contingency arrangements in designing their cash contingency arrangements.

Norges Bank is researching central bank digital currencies (CBDCs)
Norges Bank is assessing whether central bank money should also be issued in digital form. This is because cash usage is falling and the Bank is motivated by the precautionary principle, in case the monetary and payment system evolves in an undesirable direction. Further work is planned including experimental testing of technical solutions.



Initiative for regulating crypto-assets
Norges Bank supports the European Commission's initiative to remedy the lack of regulation of crypto-assets. Greater use of crypto-assets may impact the security and efficiency of the payment system. Central banks should therefore monitor developments and consider whether measures are needed.

Financial Infrastructure Report 2021
Norges Bank

Address: Bankplassen 2
Post: P.O. Box 1179 Sentrum, N-0107 Oslo, Norway
Phone: +47 22 31 60 00
Fax: +47 22 41 31 05
E-mail: central.bank@norges-bank.no
Internet: https://www.norges-bank.no

Editor: Øystein Olsen

Design: Brandlab
Layout: 07 Media AS
The text is set in 9.5 pt Azo Sans

ISSN 1894-8634 (online)

Norges Bank's *Financial Infrastructure Report*

In its annual *Financial Infrastructure Report,* Norges Bank discusses developments, vulnerabilities and risks in the financial infrastructure. The Report is a part of Norges Bank's work to promote financial stability and an efficient financial infrastructure.

Norges Bank's other reports on financial stability

In its annual *Financial Stability Report*, Norges Bank assesses vulnerabilities and risks in the financial system, with a focus on the long-term, structural features of banks, financial markets and the Norwegian economy that are of importance for financial stability.

Norges Bank's *Monetary Policy Report with financial stability assessment* includes an ongoing assessment of financial imbalances and the banking sector, Norges Bank's monetary policy assessments and the decision basis for the countercyclical capital buffer for banks.

Norway's financial system provides a comprehensive overview of Norway's financial system, its tasks and the performance of these tasks and is updated approximately every other year.

Contents

Executive Board's assessment

The *Financial Infrastructure Report* is part of Norges Bank's work to promote financial stability and an efficient and secure payment system in Norway. The Executive Board discussed the content of the *Report* on 28 April 2021.

The role and responsibility of Norges Bank for the financial infrastructure follow from the Central Bank Act. Norges Bank facilitates a secure and efficient system for settling payments and issues banknotes and coins. Norges Bank is tasked with overseeing the payment system and other financial infrastructure and contributing to contingency arrangements. Under the Payment Systems Act, Norges Bank is the supervisory authority for interbank systems.

The Executive Board considers the Norwegian financial infrastructure to be secure and efficient. There have been few disruptions in interbank systems and the securities settlement system in recent years. The financial infrastructure has also functioned smoothly during the Covid-19 pandemic.

In 2020, Norges Bank assessed three Norwegian interbank systems against international principles for financial market infrastructures (FMIs). These principles are intended to ensure a secure and efficient financial infrastructure and promote financial stability. Norges Bank consideres that the interbank systems largely comply with the principles.

There is room for improving system testing and identification of cyber incident risks. Norges Bank follows up measures to reduce the dependence on service providers of the Norwegian Interbank Clearing System (NICS), of which one requirement is that operations continue to be located in Norway.

Threats to fundamental national interests are increasingly cyber-related. According to the Norwegian Police Security Service, one of the most serious threats is digital mapping and sabotage of critical infrastructure. The financial sector is often affected more than other sectors. To improve the cyber resilience of the financial infrastructure, Finanstilsynet (Financial Supervisory Authority of Norway) and Norges Bank have drawn up a proposed framework for the independent testing of the cyber resilience of entities with responsibility for critical functions in the financial system. The proposal was circulated for comment in spring 2021.

The payment landscape is evolving. The share of cash payments is low and falling, and the Covid-19 pandemic has resulted in a further reduction in cash usage. The number of contactless payments without a PIN is rising sharply. Customers can pay at shops and online using a growing array of smartphone apps. New payment methods are often fast and user-friendly and may contribute to a more efficient payment system. At the same time, the payments market is characterised by economies of scale and network advantages, which may give individual operators undesirable market power. BigTech firms are assuming more roles in the payment system. New types of payment systems are being launched, with their own forms of money. Providers of services to banks' payment infrastructure are also becoming globalised.

The structural changes in the payment system have prompted Norges Bank to assess whether measures are needed so that the public will be able to pay efficiently and safely in NOK also in the future. Key issues are the development of the infrastructure for real-time payments, the role of cash in the future and the possible introduction of a central bank digital currency (CBDC).

Payments where the funds are available in the payee's account seconds after the payment is initiated are called real-time payments. A well-functioning real-time payment solution is an important part of an efficient payment system. In 2020, Norwegian banks began to use a new common infrastructure for real-time payments. While this is a clear advance, retail real-time services atop this infrastructure must still be improved and further developed. Norges Bank is now assessing how the infrastructure for real-time payments can best be enhanced, including whether Norges Bank should expand its operational role. This matter will be circulated for comment by industry operators and other stakeholders.

Today, nearly all payments are made using bank deposits (deposit money), money created by banks. Norges Bank issues central bank money in the form of cash. Central bank money has attributes that promote confidence in the monetary system and payment system efficiency. For central bank money to have these attributes, it must be available to and easy to use by the general public.

On 23 April 2021, the Ministry of Finance asked Finanstilsynet to draw up a draft regulation that clarifies the obligation of individual banks to ensure that customers have the opportunity to deposit and withdraw cash, either by providing their own facilities or by agreement with other cash service providers. This is in line with Norges Bank's assessment that banks' responsibilities for cash services in a normal situation should be clarified in a regulation, most recently based on a survey of banks' provision of cash services in spring 2021.

Effective electronic contingency arrangements are crucial for ensuring that the payment system can be restored quickly after a disruption. Cash is a part of overall contingency preparedness in the event of a disruption in electronic contingency arrangements. Under the Financial Institutions Regulation, banks may take into account electronic contingency arrangements in designing their contingency arrangements for cash. Norges Bank is of the opinion that how banks may do this should be specified.

Norges Bank and a number of other central banks are assessing whether central bank money should also be issued in digital form. Norges Bank's research is motivated by falling cash usage and the precautionary principle. Norges Bank wishes to be prepared to introduce a CBDC if the monetary and payment system evolves in a different direction from the one currently foreseen. A Norges Bank working group has assessed the characteristics a CBDC must have, relevant technical solutions and the impact on banks of introducing a CBDC. The research into CBDCs and developments in the monetary and payment system have shown the importance of pursuing this work further. Against this background, the Executive Board has decided to continue this research for a fourth phase of up to two years. This phase is to comprise experimental testing of technical solutions in combination with further analysis of the need for and consequences of introducing a CBDC. This work is intended to provide a basis for deciding whether Norges Bank will test a preferred technical solution. Any decision to introduce a CBDC will require a political decision. The question may also arise as to whether the introduction of a CBDC would require an amendment to the Central Bank Act.

The international messaging standard ISO 20022 will be the standard for payment messages in Norway. ISO 20022 enables messages to contain more information and structures the information in a way that facilitates more automated processing of payments. There is ongoing work at banks, Bits and Norges Bank to introduce ISO 20022. It is important that payment infrastructure participants prioritise this work.

The European Commission has taken the initiative to regulate cryptocurrencies in the EU/EEA. The purpose is to foster innovation, safeguard financial stability and protect investors. The initiative is primarily aimed at the issuance of crypto-assets and provision of services associated with crypto-asset transactions. Regulation in this area is currently lacking, and Norges Bank welcomes the initiative. Use of crypto-assets as a means of payment raises further regulatory issues that must be solved at national and supranational level. Rules for ownership rights and the transfer of such rights must be established, and rules for clarifying liability are needed. If a large number of participants – especially financial sector participants – are exposed to crypto-assets, a sudden fall in value may have systemic consequences. Increased use of crypto-assets may also be important for the safety and efficiency of the payment system. Central banks and other authorities should therefore monitor developments and assess whether there is a need to mitigate risks associated with crypto-assets.

Norges Bank's responsibility

Norges Bank is tasked with promoting financial stability and an efficient and secure payment system.[1] The Bank's tasks in this regard comprise:

- Overseeing the payment system and other financial infrastructure and contributing to contingency arrangements.
- Supervising interbank systems.
- Providing for a stable and efficient system for payment, clearing and settlement between entities with accounts with Norges Bank.
- Issuing banknotes and coins and ensuring their efficient functioning as a means of payment.

As operator, Norges Bank ensures efficient and secure operating platforms and sets the terms for the services the Bank provides. As supervisory authority, Norges Bank sets requirements for licensed interbank systems. Through its oversight work, Norges Bank urges participants to make changes that can make the financial infrastructure more efficient and secure.

The use of instruments in different areas will vary over time and be adapted to developments in the payment system and the financial infrastructure. Norges Bank is tasked with giving advice to the Ministry of Finance when measures should be implemented by bodies other than the Bank in order to meet the objectives of the central bank.

The financial infrastructure

The financial infrastructure can be defined as a network of systems, called financial market infrastructures (FMIs) that enable users to perform financial transactions. The infrastructure must ensure that cash payments and transactions in financial instruments are recorded, cleared and settled and that information on the size of holdings is stored.

Virtually all financial transactions require the use of the financial infrastructure. Thus, the financial infrastructure plays a key role in ensuring financial stability. The costs to society of a disruption in the financial infrastructure may be considerably higher than the FMI's private costs. The financial infrastructure is therefore subject to regulation, supervision and oversight by the authorities.

The financial infrastructure consists of the payment system, the securities settlement system, central counterparties (CCPs), central securities depositories (CSDs) and trade repositories.

1 Sections 1-2 and 3-3- of the Central Bank Act and Section 2-1 of the Payment Systems Act.

Norges Bank's supervision and oversight work

Oversight entails monitoring FMIs, following developments and acting as a driving force for improvements. This work enables Norges Bank to recommend changes that can make the payment system and other FMIs more secure and efficient. An efficient payment system carries out payment transactions swiftly, at low cost and tailored to users' needs.

Recommendations for making improvements may take place directly with FMIs, or through Norges Bank's external publications and speeches, targeted at both private entities and other authorities.

Finanstilsynet (Financial Supervisory Authority of Norway) supervises systems for payment services. These are retail systems, which the public has access to, such as cash, card schemes and payment applications. Norges Bank's oversight covers the payment system as a whole, including the retail systems Finanstilsynet supervises.

Even though Norges Bank oversees the payment system as a whole, individual systems are subject to regular individual oversight (Table 1).

Norges Bank is the licensing and supervisory authority for the part of the payment system called interbank systems. These are systems for clearing and settling transactions between credit institutions. If a licensed interbank system is not configured in accordance with the Payment Systems Act or the licence terms, Norges Bank will require that the interbank system owner rectify the situation. The purpose is to ensure that interbank systems are organised in a manner that promotes financial stability. Licensed interbank systems are shown in Table 1. Norges Bank may grant exemptions from the licensing requirement for interbank systems considered to have no significant effect on financial stability.

Norges Bank assesses the FMIs that are subject to supervision and oversight in accordance with principles drawn up by the Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO). The CPMI is a committee comprising representatives of central banks, and IOSCO is the international organisation of securities market regulators. The objective of the principles is to ensure a robust financial infrastructure that promotes financial stability.

Definitions in the Payment Systems Act

Payment systems are interbank systems and systems for payment services:

> *Interbank systems* are systems for the transfer of funds between banks with common rules for clearing and settlement.
>
> *Systems for payment services* are systems for the transfer of funds between customer accounts in banks or other undertakings authorised to provide payment services

Securities settlement systems are systems based on common rules for clearing, settlement or transfer of financial instruments.

A number of the FMIs that Norges Bank supervises or oversees are also followed up by other government bodies. The oversight of international FMIs that are important for the financial sector in Norway takes place through participation in international collaborative arrangements.

A detailed description of the FMIs supervised or overseen by Norges Bank is provided in *Norway's financial system* 2020.[2]

Table 1 FMIs subject to subject to supervision or oversight by Norges Bank

	System	Instrument	Operator	Norges Bank's role	Other designated authorities
Interbank systems	Norges Bank's settlement system (NBO)	Cash	Norges Bank	Supervision (Norges Bank's Supervisory Council) and oversight	Supervision: Norwegian National Security Authority
	Norwegian Interbank Clearing System (NICS)	Cash	Bits	Licensing and supervision	
	DNB's settlement bank system	Cash	DNB Bank	Licensing and supervision	Licensing and supervision of the bank as a whole: The Ministry of Finance and Finanstilsynet
	SpareBank 1 SMN's settlement bank system	Cash	SpareBank 1 SMN	Oversight	Licensing and supervision of the bank as a whole: The Ministry of Finance and Finanstilsynet
	CLS	Cash	CLS Bank International	Oversight in collaboration with other authorities	Licensing: Federal Reserve Board Supervision: Federal Reserve Bank of New York Oversight: Central banks whose currencies are traded at CLS (including Norges Bank)
Securities settlement systems	Norwegian securities settlement system	Securities and cash	Euronext VPS	Oversight	Supervision: Finanstilsynet
	VPS's central securities depository (CSD) function	Securities	Euronext VPS	Oversight	Licensing: Ministry of Finance Supervision: Finanstilsynet
	SIX x-clear's central counterparty system	Financial instruments	SIX x-clear	Oversight in collaboration with other authorities	Supervision: Swiss financial supervisory authority Oversight: Swiss National Bank, Finanstilsynet and Norges Bank
	LCH's central counterparty system	Financial instruments	LCH	Oversight in collaboration with other authorities	Supervision: Bank of England Oversight: EMIR College and Global College (including Norges Bank)
	EuroCCP's central counterparty system	Financial instruments	EuroCCP	Oversight in collaboration with other authorities	Supervision: Dutch central bank Oversight: EMIR College (including Norges Bank)

2 Norges Bank (2020a).

1 Central bank money

Today, nearly all payments are made using bank deposits, ie money created by banks. Norges Bank issues central bank money in the form of cash. Cash provides the general public with access to credit risk-free money, contributes to competition in the market for means of payment and payment instruments, and is a part of the contingency arrangements in the event of a disruption in electronic contingency arrangements. In spring 2021, on behalf of the Ministry of Finance, and in collaboration with Norges Bank, Finanstilsynet has surveyed banks' provision of cash services and assessed whether there is a need for measures or regulatory changes. Norges Bank is considering whether there will also be a need in the future to provide the public with a central bank digital currency (CBDC) to ensure an efficient and secure payment system and confidence in the monetary system.

1.1 Cash

The share of cash payments is low and falling, and the Covid-19 pandemic has resulted in a further reduction in cash usage.

Cash is issued by Norges Bank. It is important that central bank money is available to and easy to use by the general public. Today, cash is the only form of central bank money available to the general public. On 23 April 2021, the Ministry of Finance asked Finanstilsynet to draw up a draft regulation that clarifies the obligation of individual banks to ensure that customers have the opportunity to deposit and withdraw cash, either by providing their own facilities or by agreement with other cash service providers.[3]

Under the Financial Institutions Regulation, banks may take into account electronic contingency arrangements in designing their cash contingency arrangements. Norges Bank is of the opinion that how banks may do this should be specified.

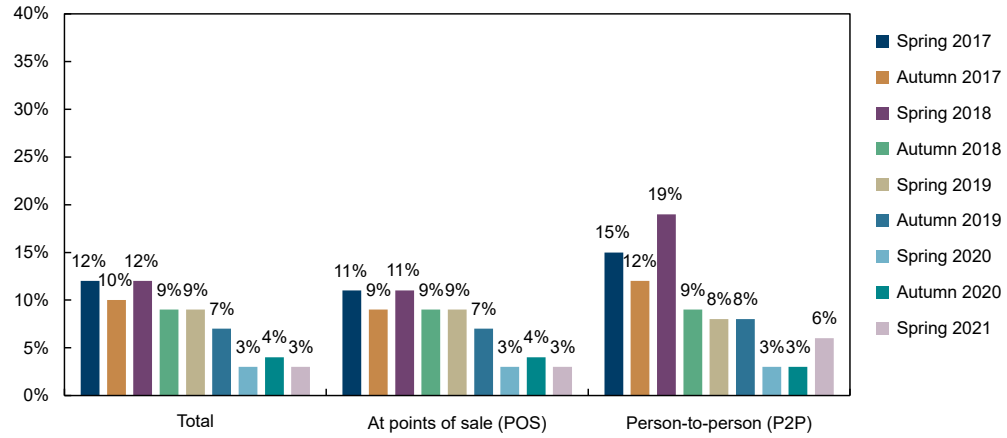
Provision of cash services

Most people make payments electronically. The share of cash payments is low and falling, both because an increasing number opt to pay electronically at physical points of sale or transfer funds electronically to other private individuals and because a greater share of overall shopping takes place online where cash cannot be used. Surveys conducted by Norges Bank indicate that the share of cash is around 3% of point-of-sale payments and somewhat higher for payments between private individuals (person-to-person) (Chart 1). Cash usage may vary by merchant type, and in the grocery trade, for example, cash usage may be higher than these data indicate. The chart shows that cash usage has declined during the Covid-19 pandemic.

On a number of occasions, Norges Bank has advocated that money issued by the central bank should be available to and easy to use by the general public. This is because central bank money has attributes that contribute to confidence in the monetary system and

3 Norwegian Government (2021).

Chart 1. Cash usage as a percentage of payment types. Number of payments



Source: Norges Bank

payment system efficiency. Central bank money gives the general public access to credit risk-free money and promotes competition in the market for means of payment and payment instruments. Central bank money in the form of cash is part of the payment system's contingency arrangements if the electronic contingency arrangements fail. For the time being, cash is the only form of central bank money available to the general public, but Norges Bank is considering whether it may also be necessary to give the general public access to a CBDC (see Section 1.2 Central bank digital currencies).

Banks are responsible for providing their customers with cash services. These include withdrawal and deposit services for both retail and business customers. In spring 2021, Finanstilsynet, on behalf of the Ministry of Finance and in collaboration with Norges Bank, conducted a survey of banks' cash services and assessed whether measures or regulatory changes are necessary. The survey comprised collection of data from banks and other providers of cash services, in addition to meetings with a number of private and public sector market participants in this area.

Provision of cash services in a normal situation

Norges Bank submitted its assessment of developments in the provision of cash services in a letter of 25 February 2021 to Finanstilsynet and the Ministry of Finance. Compared with 2018, when a similar assessment was performed, developments in access to cash services have been positive, and some of the vulnerabilities identified at that time have been reduced. Some shortcomings remain, and some new vulnerabilities have arisen. Norges Bank stands by its previous assessment that banks' obligation to offer cash services in a normal situation needs to be clarified in a regulation.

In the past three years, considerable changes have taken place in banks' provision of cash services. The number of branches offering counter cash services has been reduced, and DNB's post-in-shop cash services were discontinued in 2020. Automated services in the form of ATMs, night safes and cash deposit machines have also been reduced since 2018. On the other hand, a new in-store cash service has been established allowing customers of many NorgesGruppen grocery stores across Norway to make cash deposits and withdrawals. The service requires use of a BankAxept payment card. A majority of banks have affiliated with this service.

Retail customers' access to withdrawal services is generally satisfactory. The in-store cash service represents an improvement over cashback in connection with a purchase, since there are higher withdrawal limits and customers can withdraw cash without having to make a purchase. In some areas or municipalities, the general public does not have access to cash withdrawal services, whether through an in-store cash service, bank branches or ATMs. Nevertheless, the general public in these locations may have access to cashback in connection with a purchase. Offering such withdrawals is wholly voluntary on the part of the individual merchant, and there is no overview of merchant locations offering cashback at any given time. The reduction in the number of bank branches with cash services indicates some weakening in business customers' access to cash (change), and these customers will largely be dependent on purchasing services from other providers.

A vulnerability that Norges Bank has identified previously has been that parts of withdrawal services (cashback) have been provided by agents that are not obligated to do so by law or do not have an agreement with banks. Affiliated banks are committed to the in-store cash service, which reduces this vulnerability. At the same time, a number of banks are planning further reductions in the number of branches. This may make access to cash more difficult for persons who do not have or cannot use a payment card.

Access to deposit services by retail and business customers with small volumes of cash has improved since 2018 and is generally satisfactory where in-store cash services are available. Access by business customers with larger volumes of cash appears to be reduced and not satisfactory. This is due to a reduction in branches with cash services and in the number of night safes. The in-store cash service cannot be regarded as a full service for larger business customers because of the relatively low amount limits and because deposits must be made by feeding cash into the shop's cash register banknote feeder. The ability for business customers to make deposits must be viewed in the context of their obligation to accept cash as legal tender.

Banks appear to interpret statutory and regulatory requirements differently, regarding which banks the requirements apply to and what the requirements entail. Norges Bank stands by its assessment in the letters of 20 February 2019 and 13 February 2019 that banks' obligation to provide cash services in a normal situation needs to be clarified in a regulation.

In the 2021 *Financial Markets Report*, the Ministry of Finance writes:

> "The Ministry of Finance is of the view that the obligation to provide cash depositing and withdrawal services should be clarified, and has therefore asked Finanstilsynet to prepare a proposal for regulatory provisions requiring each bank to ensure that customers are able to deposit and withdraw cash, either under the auspices of the bank itself or through agreements with other cash service providers. Such a regulation will thus apply the principle enshrined in the 2019 *Financial Markets Report*."

The Ministry of Finance also notes that Finanstilsynet proposes the appointment of a public commission to examine the future role of cash in society and the most efficient ways to meet various customer groups' needs for cash services. The Ministry of Finance will assess the need for such a commission, *inter alia* in the light of the work of the Ministry of Justice and Public Security on consumers' right to pay cash pursuant to the Financial Contracts Act.

In order to perform its functions in the payment system and contribute to efficiency, it is important that cash is both available and easy to use. This means ensuring that the general public has real opportunities to obtain and use cash.

Provision of cash services in a contingency situation
Effective electronic contingency arrangements are crucial for ensuring that the payment system can be restored quickly after a disruption. Cash usage has fallen considerably in recent years, and electronic payment methods are becoming increasingly dominant. The consequences of a disruption in electronic payment systems may thus potentially be more extensive than before. Cash is a part of overall contingency preparedness in the event of a disruption in electronic contingency arrangements. On the basis of a proposal from Finanstilsynet and Norges Bank, on 17 April 2018, the Ministry of Finance issued a regulation that clarifies banks' responsibility to distribute cash to the public in a contingency situation.

Now that banks increasingly provide cash through in-store cash services, the availability of cash services in the event of a disruption in the electronic systems appears to have declined since 2018. In-store cash services will not be available if the systems fail and point-of-sale terminals are offline, and customers currently have fewer alternatives in the form of bank branches and ATMs.

Under the Financial Institutions Regulation, banks must adapt their cash contingency arrangements to documented and quantified assessments of the risk of increased demand for cash. Banks may take into account electronic contingency arrangements in determining the size of their cash contingency arrangements, enabling them to reduce costly demand for cash by building up electronic contingency arrangements. Norges Bank is of the opinion that objective and verifiable criteria should be established for banks' adaptation of cash contingency arrangements.

1.2 Central bank digital currencies

Norges Bank has decided to continue its research into central bank digital currencies (CBDCs) for a fourth phase of up to two years, which is to comprise experimental testing of technical solutions and further analysis of purposes and consequences of introducing a CBDC.

A CBDC is a digital form of central bank money denominated in the official unit of account for general purpose users. A CBDC can take several forms with different characteristics, depending on its purpose.

Norges Bank and many other central banks are evaluating the introduction of a CBDC. A survey by the Bank for International Settlements (BIS)[4] has found that 86% of central banks in a broad-based sample are currently studying CBDCs, and that 60% are assessing technical solutions. Several central banks, including Sveriges Riksbank and the People's Bank of China, are running pilot projects. However, only a few central banks have introduced or are about to introduce a CBDC.

Central banks have different reasons for considering the introduction of a CBDC. In emerging economies, the focus is on financial inclusion and efficient payments. In

4 Boar and Wehrli (2021).

advanced economies, the focus is more on the role of cash and the emergence of new monetary and payment systems.

For Norges Bank, the paramount question is whether introducing a CBDC is an appropriate measure for promoting an efficient and secure payment system and confidence in the monetary system.

A trend specific to Norway and some neighbouring countries is the low and falling level of cash usage. Users increasingly use payment cards with or without a PIN and pay via smartphone apps. These solutions use bank deposits as the means of payment.

At the same time, cash has some unique characteristics that could be important to preserve in the payment system of the future.

- Cash is part of the contingency arrangements if the electronic contingency solutions fail.

- Cash is a credit risk-free alternative to bank deposits and can promote competition in the payment market.

- Cash is legal tender that is widely accessible.

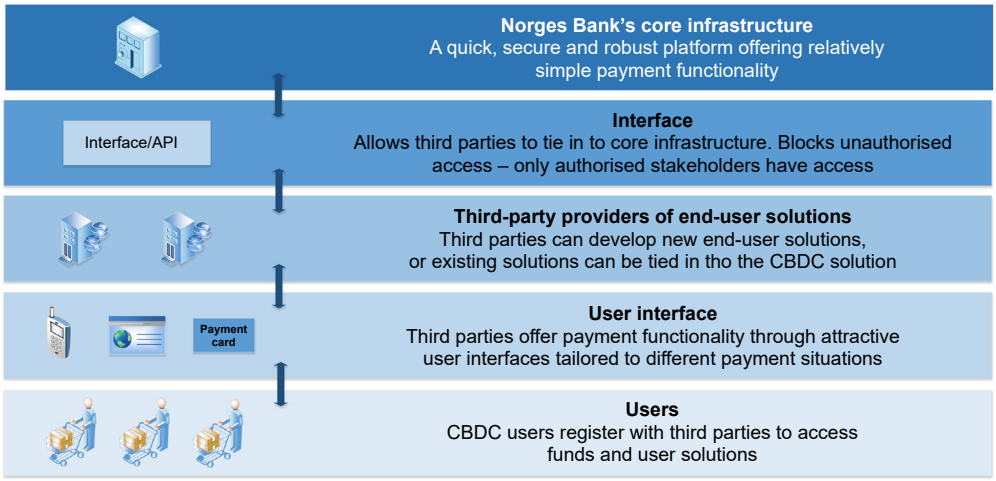
These are characteristics that are important to society, but that the individual user does not necessarily prioritise in their choice of payment solution. The question may therefore be whether any of the attributes of cash should be retained and developed further by issuing a CBDC.

In addition to falling cash usage, Norges Bank's research into CBDCs is motivated by the precautionary principle. Norges Bank wishes to be prepared to introduce a CBDC if the monetary and payment system evolves in a different direction from the one currently foreseen.

The Bank must take into account changes in the payment solutions on offer, with different forms of money. One development is the launch of stablecoins, ie cryptocurrencies designed to have a stable value relative to national currencies or other benchmarks. One example is the new monetary and payment system Diem (previously called Libra), whose backers include Facebook. The introduction of new private digital money is unlikely to have material consequences for the Norwegian monetary and payment system in the near term. Nevertheless, such initiatives illustrate the potential impact of new technologies and new user needs on the function of money in the future and raise questions about who should be meeting such needs and performing such functions. Furthermore, the Bank must take into account structural changes in banks' payment infrastructure. Norges Bank is assessing the possible consequences of these changes for competition, contingency preparedness and national governance and control of the payment system.

Norges Bank's research into CBDCs has run for a good four years. Any introduction of a CBDC will still lie some time in the future. The time spent reflects Norges Bank's view that there is no immediate need to introduce a CBDC. This is a new and complex issue, and there is little international experience to draw on. There is therefore a need for more information to be able to conclude whether introducing a CBDC is an appropriate measure. Introducing a CBDC will be such a substantive change that it will require a political decision. The question may also arise as to whether the Central Bank Act will need to be amended.

Chart 2: Overview of CBDC system architecture



Source: Norges Bank

Norges Bank has now completed the third phase of its research into CBDCs. In Norges Bank (2021), a Norges Bank working group has assessed the characteristics a CBDC must have, relevant technical solutions and the consequences of introducing a CBDC.

To the extent possible, a CBDC must be designed to fit the purpose and avoid unintended consequences. A technical solution will often deliver most of the characteristics a CBDC must have. In some cases, trade-offs between partially conflicting characteristics will have to be made. An example is Norges Bank's need to control the system, while opening it up to third parties in order to foster innovation.

Norges Bank must have control of the core of the system: the issuance and destruction of money, the register/account system and the rules. Banks and other third parties may provide end-user services. Chart 2 shows a general overview of how a CBDC can be organised (see also Norges Bank (2021)).

The working group has assessed how the features a CBDC must have can be delivered in two main categories of solutions:

- *Account-based money,* the value of which is linked to a balance in an account belonging to an identifiable account holder, with identity confirmation required for account access. This is comparable to payments using bank deposits or certain forms of e-money such as PayPal.

- *Token-based money,* where each token has a nominal value. This can be regarded as a digital variant of banknotes and coins. Funds are not associated with a named account. An electronic wallet gives a holder access to the funds. Users are linked together in a system, either directly or through a bank or another service provider. Settlement takes place when the funds are transferred between individual network participants.

Hybrids of the two main categories, solutions with elements of both, are also relevant. The working group has looked at solutions used in CBDC testing in other countries and

in cryptocurrency systems and different account-based solutions. Testing technical solutions is necessary in order to shed light on how the necessary characteristics of a CBDC can be achieved.

The potential consequences of a CBDC for the financial system depend on how the CBDC is designed. The design can affect which claims the general public chooses to replace with a CBDC and to what extent. If a CBDC replaces cash, banks' balance sheets will be unaffected – the general public will simply swap one claim on the central bank for another. If the general public replaces bank deposits with a CBDC, the consequences for the financial system may prove to be greater. Banks' access to deposit funding may be reduced, and their funding costs may rise. A guiding principle of the study is that the existence and size of any CBDC should not materially undermine private sector provision of credit to firms and households.

During financial crises or in other situations of considerable uncertainty, there may be sudden withdrawals of bank deposits by the general public. Such bank runs may lead to financial instability. Not facilitating sudden, large withdrawals from the banking sector is an important consideration in the design of any CBDC system. In the study, the emphasis is on the CBDC's function as a means of payment and payment system, rather than its function as a store of value. The study also examines various frictions between bank deposits and a CBDC that may limit the volume of CBDC and the risk of sudden changes in its volume.

Norges Bank has recently decided to continue its research into CBDCs for a fourth phase of up to two years, which is to comprise experimental testing of technical solutions and further analysis of purposes and consequences of introducing a CBDC.

The purpose of technical testing is to shed additional light on how solutions can deliver the necessary characteristics of a CBDC, and to uncover potential unintended consequences. Testing can also reveal economic and regulatory issues that are not captured by purely analytical work. In the testing phase, Norges Bank will seek to make use of experience from testing by other central banks and collaborate with them wherever appropriate. Norges Bank will draw on external providers in its technical testing work. The project phase is to provide a basis for deciding whether Norges Bank will test a preferred solution.

2 Cyber resilience

Threats to fundamental national interests are increasingly cyber-related. Serious threats include digital mapping and sabotage of critical infrastructure. Cyber crime against financial institutions is on the rise. The financial sector has been hit by cyber attacks more often than other sectors during the Covid-19 pandemic.

In 2018, the European Central Bank (ECB) published a framework for testing cyber resilience (TIBER-EU) to strengthen the cyber resilience of the financial sector and promote financial stability. In spring 2021, Norges Bank and Finanstilsynet (Financial Supervisory Authority of Norway) circulated for comment a proposal on how this framework could be introduced in Norway.

In 2020, the International Monetary Fund (IMF) published a number of recommendations on how Norges Bank and Finanstilsynet could improve cybersecurity risk supervision and oversight of the financial infrastructure. Norges Bank will follow up the IMF's recommendations.

Developments in the threat landscape and potential consequences of cyber attacks

Threats to fundamental national interests are increasingly cyber-related. One of the most serious threats is cyber mapping and sabotage of critical infrastructure. Cyber crime against financial institutions is increasing in prevalence, and during the Covid-19 pandemic, the financial sector has been hit by cyber attacks more often than other sectors. The cyber attack on SolarWinds, a company that makes ICT infrastructure monitoring tools, has shown that the potential for damage is substantial and that risk posed by software providers needs to be carefully assessed. The threat actor behind the SolarWinds attack gained access to the company's software and then inserted a compromised software update, creating a "backdoor". The software update with this backdoor was distributed to many thousands of customers and used to steal login information in order to spy on other companies. Although the attack was not directly targeted at the financial infrastructure, the experience gained from this incident is relevant and should be used as a basis for improving cyber resilience in this area too.[5]

Cyber attacks on the financial infrastructure can lead to disruptions or delays in transactions and the loss or manipulation of sensitive information. An attack can have consequences for financial stability if it disrupts critical payment system functions. A possible consequence of a cyber attack is that ICT systems no longer function or cannot be used because the system operator can no longer be certain that the data are correct. As a result, payments cannot be executed.[6] A disruption of the payment system would fairly quickly have an impact on financial stability.

Financial market infrastructures are responsible for the cyber resilience of their systems. At the same time, cyber attacks on an individual system can have consequences for other parts of the financial infrastructure and, at worst, for the entire financial system. Regulation and coordination are therefore needed. There is broad global political con-

5 Norwegian Police Security Service (2020), BIS (2021a) and National Security Authority (2020).
6 ESRB (2020).

sensus that the cyber resilience of the financial sector should be strengthened.[7] As Norges Bank is engaged in combatting the risk to the financial system posed by cyber attacks, the Bank has a wider perspective in this work that goes beyond the supervision and oversight of individual systems.

Framework to test cyber resilience in order to strengthen financial stability

In 2018, the ECB published a framework for testing how effectively a financial sector entity can detect and respond to a cyber attack, the threat intelligence-based ethical red teaming (TIBER-EU) framework. TIBER-EU is a set of guidelines that each jurisdiction can choose to implement. The purpose of the framework is to enhance the cyber resilience of financial sector entities and thus promote financial stability. The adoption of the TIBER-EU framework is not a statutory requirement.

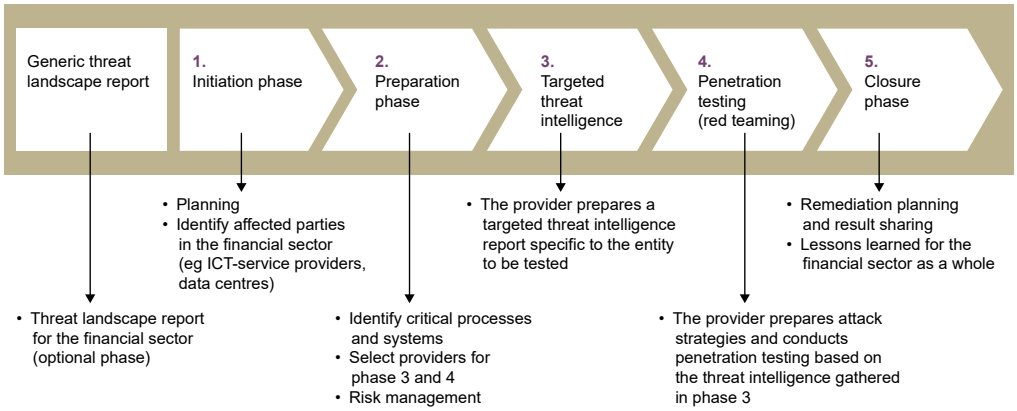
The TIBER framework sets out systematic cyber resilience testing requirements. The tests are not limited to ICT systems and technical defence mechanisms, but also apply to processes, skills and contingency plans. Entities that undergo a TIBER-EU test will largely experience the test as a real-life cyber attack.

TIBER-EU requires testing to be conducted by external red team (RT) providers. The RT provider executes a controlled attack using defined threat scenarios based on intelligence about real-life threats and vulnerabilities. The test is meant to simulate a real-life cyber attack. Only a small group of people from the entity to be tested know about the test. A standardised test format ensures quality and enables comparison of test results. The framework permits mutual recognition of TIBER tests by the different jurisdictions.

TIBER testing strengthens cyber security by providing entities with a better basis for implementing relevant measures to reduce vulnerabilities and increase cyber resilience. TIBER testing also provides better insight into cyber attack vulnerabilities and more knowledge about the extent to which these vulnerabilities can lead to systemic risk and pose a threat to financial stability.

According to the TIBER-EU framework, an implementation guide should be drawn up so that each jurisdiction adopting the framework can adapt it to suit its specificities. Norges Bank and Finanstilsynet have drafted such an implementation guide for the introduction of TIBER testing in Norway (TIBER-NO). TIBER-NO was circulated for comment in spring

Chart 3: TIBER-EU test process



Sources: Danmarks Nationalbank (2018) and ECB (2018)

7 European Commission (2019).

2021. As part of the work to prepare TIBER-NO, dialogue meetings are held with the financial sector and relevant authorities.

Under the TIBER-NO proposal, Finanstilsynet and Norges Bank will collaborate on the implementation and adoption of the TIBER framework in Norway and establish the necessary forums for overarching monitoring and governance. According to the proposal, Norges Bank will organise and staff a TIBER-NO Cyber Team (TCT-NO), which will manage and operationalise TIBER-NO, and have the formal responsibility for managing the TIBER-NO framework. This responsibility implies following up to ensure that critical functions in the financial system are tested and that testing meets the TIBER-NO requirements. TIBER-NO testing is not expected to be conducted until 2022 at the earliest.

The European Commission published its proposal for a Digital Operational Resilience Act (DORA) for the financial sector in 2020. DORA sets cyber resilience requirements, including requirements for regular threat-led testing, and is expected to be transposed into Norwegian law as a regulation. It may be necessary to adjust TIBER-NO when DORA enters into force.

Recommendations from the IMF on further improving cyber security risk supervision and oversight of the financial infrastructure

In 2020, the IMF conducted an assessment of cyber resilience in Norway's financial sector.[8] The assessment was part of a comprehensive review of the Norwegian financial system. The IMF regularly carries out assessments of financial stability among member countries in its Financial Sector Assessment Program. The IMF's recommendations to Norges Bank on further improving cyber resilience are related to processes for cybersecurity risk oversight, Norges Bank's expectations of payment system operators, reporting of potentially critical incidents and the need to strengthen the Bank's oversight function in this area.

In the period ahead, Norges Bank will increase its focus on cyber resilience in its oversight of the financial infrastructure and set clearer cyber resilience requirements for payment system operators. Operators are expected to conduct self-assessments of their level of maturity based on internationally recognised standards, set goals and implement measures to achieve these goals.

8 IMF Country Report Norway 2020.

3 Interbank systems

Norges Bank is both operator and licensing and supervisory authority for a part of the financial infrastructure called interbank systems. These are systems for clearing and settling payments between credit institutions.

Norges Bank published an assessment of three Norwegian interbank systems against international principles for financial market infrastructures (FMIs) in 2020. The principles are designed to ensure that FMIs are robust and efficient and to promote financial stability. In Norges Bank's assessment, the systems are broadly in compliance with the principles.

Norwegian banks started to use a new common interbank infrastructure for real-time payments called NICS Real in 2020. Real-time payments are payments where the money is made available on the payee's account seconds after payment is initiated. Norges Bank is now considering whether NICS Real should be further developed or be replaced by an infrastructure offered by the central bank. One objective is to promote the use and development of new retail real-time payment services. The matter will be circulated for comment to the industry and other stakeholders.

Operation and development of FMIs has largely been outsourced. ICT service providers are thereby crucial for the delivery of critical functions for the payment system and other FMIs. There have been substantial changes over the past year in the situation regarding service providers for the Norwegian Interbank Clearing System (NICS), one of the most important interbank systems in Norway.

3.1 Assessment of interbank systems against international principles

Norges Bank assesses FMIs against the Principles for Financial Market Infrastructures issued by the Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO).[9] The CPMI is composed of representatives from central banks, and IOSCO is the international organisation for securities regulators. The principles are designed to ensure that FMIs are robust and efficient and promote financial stability. The principles provide a unified set of standards for FMIs across national borders and different systems.

Norwegian system operators first performed self-assessments against the FMI principles in 2013. Norges Bank assessed the systems in 2014 based on operators' self-assessments and other information.[10] Since 2015, Norges Bank has regularly reassessed the systems against principles that have not been fully observed and against other principles when changes were made to the systems.

Norges Bank conducted a new complete assessment of the Norwegian interbank systems NICS, DNB's settlement bank system and SpareBank1 SMN's settlement bank system

9 CPMI-IOSCO (2012).
10 Norges Bank (2014).

in the course of 2019 and 2020. Norges Bank found all the systems to be robust, and the main conclusion was that they complied with international principles.[11]

Norges Bank nevertheless made some recommendations, with particular focus on:

- *Contingency exercises.* Exercises should be conducted regularly and should test the most important contingency functions. A sufficiently large portion of the organisation should be involved so that the exercises include different aspects of crisis management. In particular, an exercise for switching from a settlement bank to Norges Bank should be conducted for level 2 banks[12]. In addition to verifying functionality, such exercises can show whether level 2 banks have sufficient liquidity (in the form of deposits or access to lending facilities) at Norges Bank to cover their positions.

- *Dependency on service providers.* ICT service providers are crucial for the delivery of critical functions for the payment system and other FMIs. In Norges Bank's view, dependencies on critical service providers should be reduced, so that switching to a different provider when necessary can be efficient and robust. Dependency on service providers is an area Norges Bank will prioritise in its supervisory and oversight work ahead.

- *ISO 20022.* The messaging format ISO 20022 is an important element in an efficient payments infrastructure (see box: Introduction of ISO 20022). In Norges Bank's view, it is important for participants to prioritise work on the transition to ISO 20022. NICS Real is ready for the transition to ISO 20022, but banks must also make their own adjustments to enable migration to the new format. The plan is for banks to have finished making their adjustments by the end of 2022. Norges Bank recommends that Bits continues to replace old national messaging formats with ISO 20022 in other parts of NICS.

In addition to assessing NICS and the DNB and SMN settlement bank systems, Norges Bank conducted a self-assessment of Norges Bank's settlement system (NBO) against the CPMI-IOSCO principles.[13]

3.2 Real-time payments

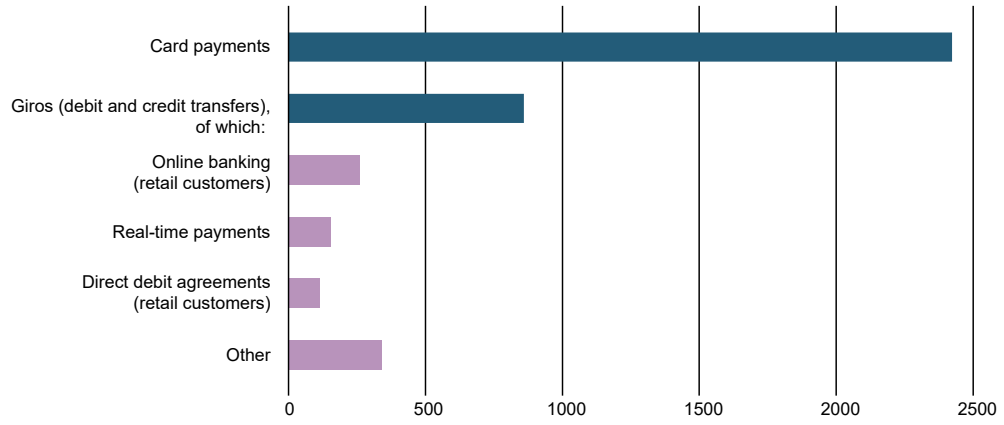
Real-time payments are payments where the money is made available on the payee's account seconds after payment is initiated. Norges Bank is currently assessing how the infrastructure for real-time payments can best be further developed, including whether Norges Bank should expand its role as operator. The issue will be circulated for comment to the industry and other stakeholders.

New common infrastructure

Owing to developments in technology and market structure in recent years, payment services have increasingly become a competitive arena. Customer contact through payment services has gained strategic importance for both banks and other participants. Such services should build on a common underlying infrastructure that is secure and fast and operates at low cost. A common infrastructure can be regarded as a collective good that benefits us all. Providers can then compete freely for customers through various applications and interfaces.

11 A detailed description of Norges Bank's assessments was published in Norges Bank (2020c).
12 Banks can participate directly in settlement at Norges Bank (level 1) or indirectly (level 2). Level 2 banks settle their positions in Norges Bank through another bank (private settlement bank).
13 Norges Bank (2020d).

Chart 4 Number of transactions carried out in 2020 by payment type
In millions of payments



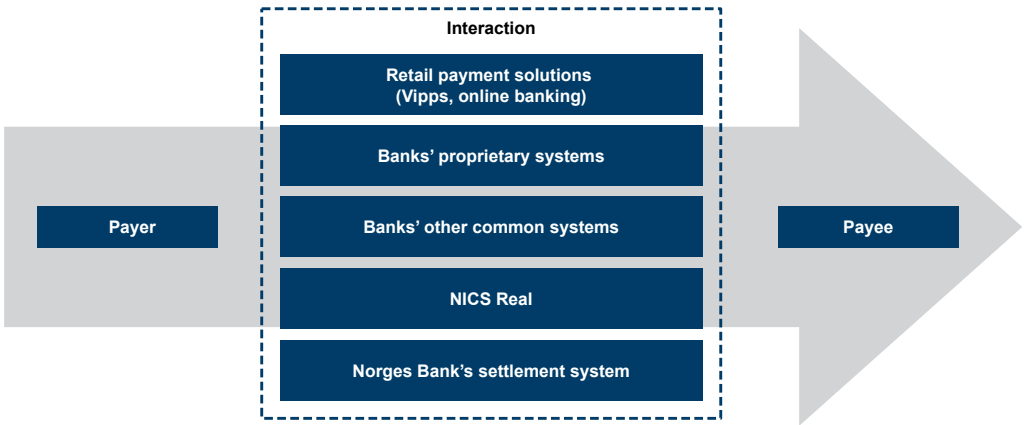
Source: Norges Bank

The banking sector established a common solution for real-time payments in 2013. The solution had some shortcomings, and it took many years before it was adopted by several of the larger banks. NICS, the banks' joint interbank system, was expanded in 2020 to include a new system for real-time payments called NICS Real. A majority of the banks have now joined. In 2020, 154m real-time payments were executed in Norway (Chart 4).

NICS Real is a clear advance on the previous solutions used by banks. Before NICS Real, the payee's account was credited before interbank settlement had been completed. The payee's bank ran the risk that the funds from the payer's bank might not arrive as agreed. This risk has now for all practical purposes been removed, with liquidity set aside at the central bank to guarantee settlement.

NICS Real is an important component of the overall infrastructure required to execute a real-time payment. A number of different participants and systems are involved. Retail payment solutions, for example, use NICS Real (Chart 5). Retail payment services are also offered by participants other than banks.

Chart 5 Simplified illustration of the real-time payments infrastructure



How well the retail services function depends to some extent on the opportunities provided by the common underlying infrastructure and on developing the infrastructure further to accommodate new kinds of services. A remaining question is how this infrastructure can best be further developed (see box: Introduction of ISO 20022).

Norges Bank's role as operator

Like a number of other central banks, Norges Bank is assessing whether to expand its role as payment system operator. NICS Real could in that case be discontinued and replaced by a system offered by Norges Bank, whereby payments would be settled directly at the central bank. In its assessment, Norges Bank will explore whether taking responsibility for a larger portion of the *underlying* infrastructure could give access to tools to promote the use of and innovation in services in the *retail* layer of the infrastructure (Chart 5). For example, in Norges Bank's view, new real-time payment services for businesses and the public sector should be developed.

There are two relevant alternatives for direct settlement of real-time payments at Norges Bank. The first alternative is to set up a system where Norges Bank is itself responsible for management, development and operation. The second alternative is to join the Eurosystem's TIPS solution, operated by the European Central Bank (ECB).[14] Payments would then be settled in TIPS in NOK on behalf of Norges Bank. The better of these two alternatives will be assessed against further development of today's solution. Under the latter alternative, NICS Real will be further developed, and the current division of responsibility between Norges Bank and the banking industry will continue to apply. Norges Bank will then continue to work for better real-time payments through its supervisory and oversight work.

14 In 2020, Sveriges Riksbank and Danmarks Nationalbank decided to join TIPS.

INTRODUCTION OF ISO 20022

ISO 20022 is an international standard for financial messaging developed by the International Organization for Standardization (ISO). Projects are in progress in the industry and at Norges Bank to replace national standards and formats with ISO 20022.

ISO 20022 messages can contain more information than today's Norwegian formats. The information is also structured in a way that facilitates a more automated payment process. In addition, there are considerable advantages to enabling solutions throughout the payments value chain to speak the same language. A message that has to be sent through systems using different formats has to be translated en route, which for example increases the level of system complexity.

The introduction of a new messaging standard is a comprehensive process. The work entails risk, costs and the need for coordination between the various participants.

The board of Bankenes Standardiseringskontor (the banks' standardisation office, now Bits) took a decision in principle in 2014 that ISO 20022 should be the standard for all payment messages in Norway. Part of the background for this decision was the EU requirement that all retail payments in EUR, including payments in the EEA area, would be required to be ISO 20022 compliant by 31 October 2016.

The part of the banks' joint interbank system (NICS) that processes real-time payments is ready for the transition to ISO 20022. In addition, Bits launched a preliminary project in late spring 2020 to prepare a basis for the modernisation of all of the NICS system. The project includes implementation of ISO 20022 in the exchange of payment transactions between the banks and the rest of NICS.

The basis for the project also included requirements set by Norges Bank regarding service provider independence. The fact that NICS is based on national messaging formats is according to Bits part of the reason why the number of potential ICT service providers for NICS is limited. The transition to ISO 20022 could thus reduce service provider dependence.

Work is now in progress at Norges Bank on a preliminary project for the transition to ISO 20022 messaging for Norges Bank's settlement system (NBO).

For payment transactions to be exchanged between the above-mentioned interbank systems and the banks in the ISO 20022 format, banks will also have to change and adjust their systems accordingly.

Irrespective of the solution that is chosen, the system for real-time payments must be efficient and robust, facilitate innovation and competition, and ensure satisfactory national governance and control. The issue will be circulated for comment to the industry and other stakeholders.

3.3 Service providers for the NICS interbank system

There have been substantial changes over the past year in the situation regarding service providers for NICS, one of the most important interbank systems in Norway. Mastercard recently acquired parts of Nets, which has provided operational services for NICS for many years. In addition, a merger has been sought between the rest of Nets and the Italian payments processor Nexi. Such changes highlight the need to reduce the risk to NICS posed by dependence on service providers.

The Norwegian Interbank Clearing System (NICS) is the banks' joint system for exchanging and clearing payment transactions. Almost all payment transactions in NOK are sent to NICS for clearing before being sent on to Norges Bank's settlement system (NBO) for settlement.

Bits AS (Bits), the Norwegian banking and financial industry's infrastructure company, is the system operator for NICS and is licensed by Norges Bank. The technical operation of NICS was outsourced to Nets Norge Infrastruktur AS (NNI), a wholly-owned subsidiary of Nets Denmark A/S, for several years. Other companies in the Nets Group also perform operational tasks for NICS.

Norges Bank received a change notification from Bits in 2019[15] concerning Mastercard's plans to acquire Nets' account-to-account services, including NNI and the NICS source code. Norges Bank approved the change notification on certain conditions. Norges Bank

15 Section 2-6 of the Payment Systems Act: The operator shall notify Norges Bank before making significant changes with respect to ownership, organisation, operations, etc, as referred to in Section 2-4 to Section 2-5.

has also previously set conditions for the operation of NICS by Bits as system operator. The conditions now include:

- Bits must have adequate capacity and expertise to manage and control operational deliveries and manage the outsourcing contract.

- Hardware for NICS' basic operations must be physically located in Norway. An operational contingency solution that can immediately take over the operational monitoring of NICS currently performed by Nets in Denmark must also be in place at all times in Norway.

- Any acquisition by Mastercard must not change Bits' access to the NICS source code.

Mastercard's acquisition was completed on 5 March 2021.[16] ICT operational services for NICS will still be performed by the part of Nets not included in the acquisition. If Mastercard wishes to choose solutions or providers other than Nets, a change notification is required to be sent to Norges Bank before the change can be made. For example, it has been reported that a merger is being sought between the remaining part of Nets and the Italian payment processor Nexi.[17] The agreement between Bits and Mastercard must comply with the conditions set by Norges Bank and ensure that Bits can perform the necessary management and control, irrespective of the service providers used for NICS.

Changes in the situation regarding service providers highlight the need to manage the risk to NICS posed by dependence on service providers, so that switching to a different service provider when necessary can be efficient and robust.[18] In connection with its assessment of the change notification regarding the acquisition of parts of Nets by Mastercard, Norges Bank set the condition in 2020 that Bits must reduce the risk of dependence on service providers to ensure that NICS can continue to be operated in Norway.[19] Bits has now launched a long-term plan to modernise NICS and increase service provider independence. An important element of this work is the transition to the international messaging format ISO 20022 for all the components of the NICS system and for the exchange of transactions between banks and NICS (see box: Introduction of ISO 20022). Bits has requested banks to provide feedback on the various measures proposed to achieve the intended modernisation of NICS by the end of April 2021.

Norges Bank will place considerable emphasis on service provider relations in its work as supervisory authority for NICS.

16 The contractual party for Bits in the outsourcing of NICS is now *Mastercard Payment Services Infrastructure (Norway) AS*.
17 The merger was approved by the European Commission on 8 March 2021.
18 See also Norges Bank (2020c).
19 The condition was set regardless of whether Mastercard's acquisition was completed.

4 Crypto-assets

Crypto-assets have received considerable attention over the past year. Professional investors have included them in their portfolios, and traditional payment service providers have made crypto-assets available to their customers both as a speculative investment and for making payments. In addition, new crypto-assets have emerged with value stabilisation mechanisms. New financial market infrastructures and services have been established for trading in assets accessible via cryptographic keys, including "decentralised finance". While there is potential for useful innovation, developments do entail risks. Money and payment systems require a number of fundamental legal rules that are often taken for granted and that have not necessarily been established for crypto-assets. This also applies to private law rules, which clarify who owns money, how ownership is transferred and the liabilities of the parties that issue money and provide payment services.

Increased interest in cryptocurrencies

Crypto-assets are units in data ledgers that are accessed using cryptographic codes and are perceived as having value as a means of payment or as services provided by the ledger. These ledgers are often based on distributed ledger technology (DLT), so that no single operator has control. Many crypto-assets are referred to as cryptocurrencies, for which there is no central operator that manages the issuance of new units and verifies transactions.

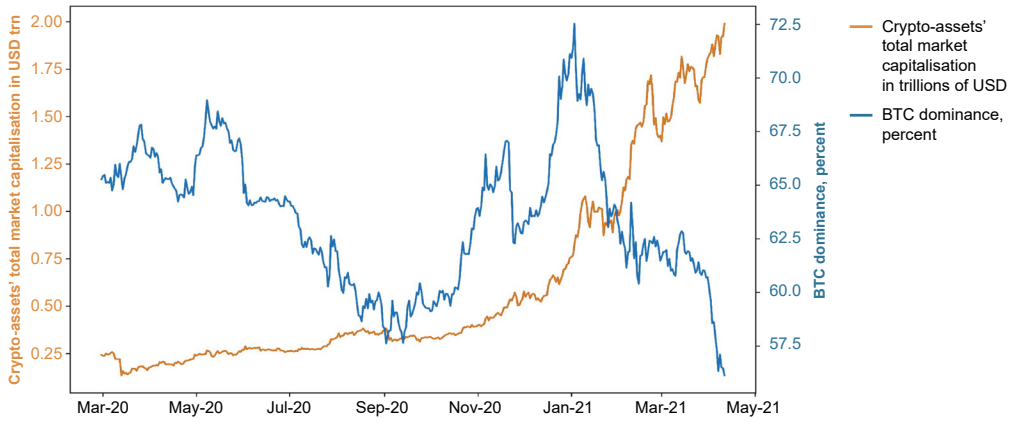
Many crypto-assets, such as Bitcoin, are based on a social consensus that only a limited number of units can be issued, so that its value fluctuates in pace with demand. This is referred to as digital scarcity. However, there is no digital guarantee limiting the number of units, nor any guarantee of demand to create scarcity. A decentralised design is no guarantee that individual operators do not have different forms of control or influence and are unable to affect design changes and operation.[20]

Crypto-assets can also provide functionalities that traditional money lacks. For example, programmability can make payments more automated and situation-dependent. These automated payments are often referred to as smart contracts. Programmable money is discussed in greater detail below. Many central banks are currently assessing whether the technology is relevant for central bank digital currencies (CBDCs), as discussed in Section 1.2 Central bank digital currencies.

Prices for many crypto-assets rose sharply in autumn 2020. Both financial and non-financial sector market participants have announced that they already have or are planning exposure to crypto-assets. They can either invest directly by purchasing crypto-assets or invest in financial instruments or businesses that provide such exposure. Moreover, mass market payment and investment apps, such as PayPal and Robinhood, have made it easier for non-professionals to invest in crypto-assets. Both Mastercard and Visa have announced support for payments using crypto-assets on their respective networks. Alongside this is the emergence of so-called decentralised finance, which makes trading possible in complex financial products based on crypto-assets. Another development is that social media are increasingly being used to influence demand for, and thus the price of, various crypto-assets.

20 Sai et al (2020).

Chart 6: Total market capitalisation of crypto-assets in trillions of USD and Bitcoin dominance ratio



Source: tradingview.com

Chart 6 shows developments in total market capitalisation of crypto-assets in the past year, together with the size of the share represented by Bitcoin (BTC) ("BTC dominance").[21] A declining share of BTC shows that much of the growth is attributable to crypto-assets other than Bitcoin.

Certain crypto-assets – so-called stablecoins – have mechanisms that help provide greater stability against national currencies or other benchmarks, for example, because the supply can be adjusted in response to changes in demand.[22] Some of these are based on a decentralised, algorithm-based stabilisation mechanism, without central operators that can influence the value for their own gain. The value of other stablecoins is kept stable by being pegged to other assets. Some stablecoins have successfully achieved a relatively stable value over a period, while others are traded at a small fraction of the value of the assets they are pegged to. Stablecoins have shown strong growth over the past year, primarily for use in crypto-asset trading and decentralised finance, but many are intended for use in more traditional payments. When stablecoins aim for a stable value against national currencies, they rely on central banks' responsibility for price stability.

If the volume of crypto-assets ever becomes substantial, the ability of central banks to perform their tasks could be affected. Flaws in the assumptions underlying the technology or in the technical architecture can result in abrupt price declines. If a large number of investors, particularly financial sector participants, expose their balance sheets to crypto-assets, abrupt price declines can have systemic consequences. Greater use of crypto-assets as a means of payment and as payment systems can also have an impact on the security and efficiency of the payment system. It has therefore become more important for central banks to monitor developments and assess whether measures are needed to reduce risks related to crypto-assets.

Regulatory initiatives

Regulations can help ensure that gains from crypto-assets and related technology are realised at an acceptable risk. In recent years, many regulatory initiatives have been taken by international government bodies.

21 These variables are calculated by tradingview.com.
22 Stablecoins are described in greater detail in Norges Bank (2019) and Norges Bank (2020b).

At the G20 meeting in June 2019, the need for regulation of so-called global stablecoins (GSCs) was on the agenda, and different international governing bodies were tasked with assessing the need to regulate them within their areas of responsibility.[23] Aims included measures to counteract the use of crypto-assets for money laundering and other criminal activity[24], and measures to promote financial stability. In October 2020, the Financial Stability Board (FSB) published recommendations for the regulation, supervision and oversight of "global stablecoin arrangements", with a particular focus on their potentially systemic role.[25]

In September 2020, the European Commission published its proposal for a regulatory package to promote digital finance in the EU.[26] This will also affect Norway, which is an EEA member country. Included in the package are rules for crypto-asset markets[27] and for financial market infrastructures (FMIs) wishing to test DLT (see box European Commission's proposed Markets in Crypto-Assets Regulation).[28]

23 For a more detailed account, see Norges Bank (2020b).
24 BIS (2021b).
25 FSB (2020).
26 The Digital Finance Package (see European Commission (2020a)).
27 MiCA (see European Commission) (2020b).
28 European Commission (2020c).

EUROPEAN COMMISSION'S PROPOSED MARKETS IN CRYPTO-ASSETS REGULATION

A main principle of the proposal is technological neutrality, ie the same activities and risks should be regulated equally, irrespective of technology. At the same time, some weight is given to particular issues and risks related to the use of crypto-assets and distributed ledger technology (DLT).

The proposed Markets in Crypto-Assets Regulation is intended to promote innovation and realise the gains of new technology while also protecting investors and consumers, and safeguarding financial stability. The regulation primarily targets issuers of crypto-assets and different service providers, such as trading platforms, custodians and advisors. In addition, there are market abuse rules. Market participants and services already subject to other regulations, such as the Securities Regulation, are not included.

Crypto-asset issuers must meet organisational requirements and provide documentation of the crypto-asset's characteristics. Stablecoins have drawn particular attention. The proposed regulation addresses two types of stablecoins: e-money tokens and asset-referenced tokens. E-money tokens are stablecoins intended to be stable against specific national currencies. Asset-referenced tokens are stablecoins designed to be stable against other benchmarks, such as a basket of currencies or the price of one or more commodities. By expanding the regulatory regime to include stablecoins considered to be "significant", the proposed regulation also addresses the possibility that stablecoins could become systemic.

The proposed Markets in Crypto-Assets Regulation is accompanied by a separate proposal for a pilot regime on DLT market infrastructures for financial instruments based on DLT to allow for experimentation. This is not a complete regulation, but permits market infrastructures to meet necessary requirements in a different way if they use DLT. This regulation can promote learning benefits for both market participants and the authorities.

The European Commission's proposed regulation primarily entails the regulation of crypto-assets as a separate asset class by regulating issuance, trading and information. Such regulation will protect investors and promote financial stability. There are many issues and risks related to crypto-assets that are not covered by the regulation. For example, the regulation does not cover liability for participants in a DLT system. The regulation disregards this issue by specifying that when new units of a crypto-asset are generated when transactions are validated using DLT, as in many crypto-asset systems, they are not considered to be issuances. Liability for activities outside the scope of the regulation must be based on general statutory rules, which can vary across countries.

Crypto-assets as a means of payment

The European Commission's proposed regulation does not cover the contractual arrangements between entities using crypto-assets as a means of payment for settlement between them.

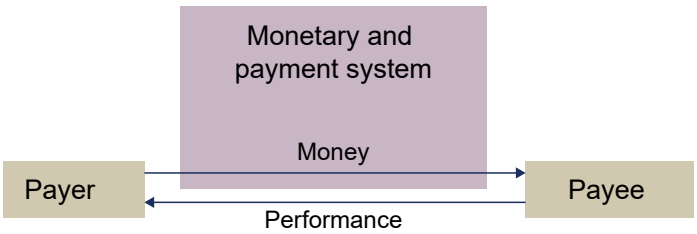
A contractual arrangement normally entails one entity that commits to payment of money and another that commits to providing a good or service (Chart 7). A stable monetary unit combined with a cost-efficient payment system help keep transaction costs low, along with rules underpinning certainty and predictability for users. In addition, this promotes financial stability, in part by preventing uncertainty surrounding a payment from having ripple effects on other payments.

The Financial Contracts Act contains provisions for the way payment is to be made and when a payment obligation is considered to be settled. The Payment Systems Act provides rules for when interbank payments are final and can therefore no longer be halted or reversed. Further, the Financial Contracts Act contains provisions on liability in the event something were to go wrong with a payment, for example when a payment instrument is misused. Many of these rules are harmonised in the EU, pursuant to the revised Payment Services Directive (PSD2) and other legislation.

The Financial Contracts Act is primarily aimed at payments that use cash or bank deposits. This implies that when other means of payment are used, such as crypto-assets, the parties involved must either resort to regulation by contract or rely on background rules of law and contract interpretation. This increases transaction costs and can create legal uncertainty as to whether a payment has been made. If crypto-assets turn out to play a greater role as a means of payment, it would be appropriate in principle for the rules to be made more technology-neutral and adapted to the use of crypto-assets as a means of payment.

However, crypto-assets as a means of payment raise a number of new issues and risks (see box Issues relating to the use of crypto-assets as a means of payment). Issues specific to crypto-assets may suggest the need for supplementary or separate rules for

Chart 7: The role of a monetary and payment system in a contractual arrangement



ISSUES RELATING TO THE USE OF CRYPTO-ASSETS AS A MEANS OF PAYMENT

Contracts for payment normally include a unit of account, for example the Norwegian krone, and a means of payment denominated in that unit of account, often bank deposits. The parties do not need to consider value fluctuations in the means of payment compared with the unit of account. Even though stablecoins have stabilisation mechanisms, the value could fluctuate and, at worst, the means of payment could lose all value. Such fluctuations complicate contractual arrangements and create risk that the parties did not previously need to consider.

When using crypto-assets, the parties must acknowledge that in many cases, such means of payment are unable to provide the same degree of finality that is provided by payments using bank deposits or cash. Crypto-asset systems often only provide probabilistic finality, which means that it cannot be completely ruled out that the ledger can be reorganised and previous payments changed, for example resulting from an attack. This can complicate the contractual arrangement as there can be disagreement regarding whether or not a payment has been made if the ledger were to be reorganised.

An important attribute of money is that it is fungible: each individual unit has the same value and is mutually interchangeable. Cash and bank deposits have attributes and are subject to regulatory frameworks that secure fungibility. For crypto-assets, a ledger history will often follow each individual monetary unit that is publicly available on an open blockchain. Different analytical techniques can also be used to inform the ledger history of each individual unit. Consequently, units may not be considered fungible by the users. For regulatory or other reasons, some users will not accept units with undesirable ledger histories. This can create situations where the payer and the payee disagree on whether payment has been made.

payments using them, in the same way that the European Commission has proposed separate rules for crypto-asset markets instead of supplementing other financial sector regulations.

User interface for crypto-asset payments

To receive and make use of crypto-assets, a user interface is needed. Typically, an interface manages a user's cryptographic codes (key), which provides control over crypto-assets. Interfaces also ensure communication with the crypto-asset system, which includes "signing" valid transactions and submitting them to the network. The interface therefore has many of the same functions as payment cards and payment applications using bank deposits.

User interfaces for the use of crypto-assets are often referred to as wallets, of which there are two main varieties.[29] **Custodial wallets** entail third-party custody of the user's cryptographic codes. The user can make use of their assets by logging in to the third party's user interface. A disadvantage of this application is that the user is susceptible to losing their crypto-assets in the event of a failure of or attacks on this operator. The user cannot simply transfer to another wallet vendor. Issues may also arise related to who owns crypto-assets protected by the keys, if this is insufficiently regulated. If users' funds "stored" in a custodial wallet become substantial in the aggregate, a disruption to

29 Karantias (2020) and Allen et al (2020a).

the wallet may have systemic consequences. Vendors of such wallets are similar to service providers that are subject to the European Commission's Markets in Crypto-Assets Regulation. These regulations are aimed at protecting the user from credit risk from service providers and promoting financial stability. It might also be necessary to further regulate private law conditions and the apportionment of liability when faults occur if such wallets are used for payments and in the event of disruptions in the same manner that providers of payment instruments are currently regulated. If crypto-assets become more widely accepted as a means of payment, it will be natural to include the regulation of wallet vendors in a revision of the Payment Services Directive (PSD2).

With the other variant – **non-custodial wallets** – users hold their own cryptographic keys locally.[30] Users of these wallets do not face counterparty risk related to the wallet vendor. In principle, such wallet vendors do not have access to users' codes and therefore cannot access users' crypto-assets. If users' keys are lost or accessed by attackers using malware, the users' funds could be lost or stolen.[31] In principle, this type of wallet is merely software that can be downloaded and used by users. Such software can be downloaded from anywhere in the world and in some instances, the identities of the developers may be unclear. In some cases, this software has been developed using open source code, making it difficult to identify individuals who can be held liable. Vendors of non-custodial wallets do not appear to be included among regulated service providers in the European Commission's proposed Markets in Crypto-Assets Regulation. Insufficient regulation can give rise to ambiguities related to the appointment and enforcement of liability for risk in the event of a failure by the vendor, such as insufficient security. This could mean that users would need to cover losses even though liability should rest with the vendor or developer. Non-custodial wallets may also enable evasion of know-your-customer rules and measures to monitor and prevent payments related to criminal activity. It is therefore necessary to explore regulatory strategies in order to protect users. Both national and international cooperation may be needed to develop good regulatory strategies.

Irrespective of technical solution, it will probably be easiest for many users to use an interface from a familiar and trusted operator that is compatible with other financial and/or digital services that the user uses. This will typically include existing payment interfaces, such as banks' user interface, Vipps or PayPal, or services integrated with payment and communications interfaces provided by BigTech companies such as Google, Apple and Facebook. A number of such market participants have added or are considering adding crypto-assets to their payment platforms. Network advantages and the ability to link the wallet to other services will give such providers a competitive advantage.

In Norges Bank (2020b), it was pointed out that BigTech firms may have a particular influence on the competition to offer payment solutions based on the traditional payment infrastructure, with possible related risks. Mobile operating system providers such as Apple and Google have a certain degree of control over what apps are available to users, for example through their control of the marketplace for apps, such as the App Store and Google Play. They can also control which apps can have access to a phone's various hardware elements. For example, Apple does not give payment apps other than Apple-Pay direct access to the NFC functionality, which is used for contactless payments. To the extent that a non-custodial wallet utilises a phone's secure elements to store codes etc, a similar situation may arise, since the secure elements are reserved for selected

30 The wallet can be based on proprietary systems for storing cryptographic keys or on more standardised solutions. Proprietary systems can make it difficult for a user to spend their crypto-assets if the vendor's system fails or, if for other reasons, the user wishes to use another interface. There are many standardised solutions for managing cryptographic keys, for example by using standardised "seeds" which essentially means that a user's keys can be generated by stringing together different words. The user must then use this string to regenerate his keys in a new wallet.

31 Different solutions exist to reduce this vulnerability. The customer has the option of storing keys on offline devices and transfer small amounts at regular intervals for online use. The customer can also use secure hardware, ie certain hardware components of the user's equipment are insulated, which makes it difficult for malware to reach.

crypto-assets. BigTech firms will therefore be able to influence which wallets are used, by also giving advantages to proprietary solutions and the crypto-assets they are involved in. This gatekeeper role can have a positive impact by steering users towards secure and legitimate solutions. The gatekeeper role can also be point of entry for regulation and liability, particularly when placing liability directly on the software vendor is difficult (cf discussion of non-custodial wallets). But the gatekeeper role can also amplify operators' market power and any systemic roles.

Work is under way in the EU to regulate digital platforms. For example, proposals include a Digital Services Act that will require certain digital platforms to protect consumers and promote competition as a supplement to the general competition rules.[32] This may address challenges related to market power, but not necessarily the financially systemic role that this market power could entail. It might also suggest that digital platforms with systemic positions should also be subject to specific requirements in order to promote financial stability.

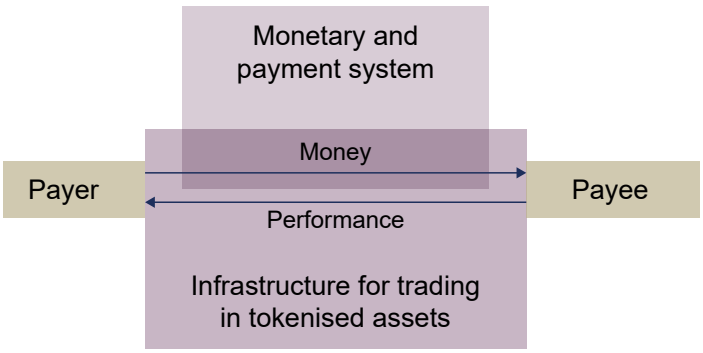
Market infrastructures for tokenised asset trading

The premise of the discussion above is that the monetary and payment infrastructure is relatively independent of the rest of a contractual relationship between parties. In large financial transactions, FMIs and other intermediaries will also ensure that payment does not take place until the contract is performed and vice versa in order to mitigate counterparty risk. In principle, however, it is beyond the function of the payment infrastructure to decide whether or not the contract is considered performed prior to execution of payment.

With so-called programmable money and tokenisation of assets, the payment system and platform where the contract is fulfilled could be more tightly integrated into what are called market infrastructures for tokenised asset trading. This is illustrated in Chart 8. Tokenisation is the process of converting assets into digital tokens, which can then be used via cryptographic codes in the same way as a crypto-asset. Programs can be written – smart contracts – for automated contract performance. For example, smart contracts can be used to ensure that assets are not transferred unless payment occurs and vice versa, in order to eliminate counterparty risk. The proposed regulation from the European Commission discussed above allows FMIs to test such technology.

Automated settlement between programmable money and tokenised assets can occur in market infrastructures that are more or less decentralised. A number of market

Chart 8: Integrated market infrastructure for money and tokenised assets



32 European Commission (2020d).

participants are experimenting with such systems. In cooperation with the Swiss National Bank and SIX, the BIS Innovation Hub has developed and tested such a market infrastructure for securities trading and settlement.[33] Funds can be entered into the market infrastructure in different ways. Money can be issued directly by a private entity or the central bank, or funds from an external ledger can be locked in, which is consolidated with this ledger according to pre-determined rules.

There are many potential benefits of such market infrastructures for automated tokenised asset trading and the use of smart contracts. For instance, settlement can occur without counterparty risk and without the need for central intermediaries. However, such market infrastructures also create new risks and a new need for regulation (see box Risks associated with market infrastructures for tokenised assets and the use of smart contracts). Property rights must be adapted to link control over assets to cryptographic keys. A number of countries have introduced legal rules that clarify fundamental rules for the content and extent of property rights to tokenised assets and their creation, termination or transfer.[34] If such rules are not harmonised at EU level, such rules should also be considered in Norway.

Market infrastructures for trading in tokenised assets can be organised and controlled by individual operators, as in the BIS Innovation Hub project discussed above. Market infrastructures for "decentralised finance" are also being developed based on DLT. Such market infrastructures often aim for decentralised governance and operation. For the time being, these market infrastructures have been primarily tested for and used for trading in different crypto-assets and related derivatives and not tokenised variants of traditional assets. Decentralised finance is described in detail in Østbye (2020).

Decentralised finance may enhance the efficiency of the financial sector and promote financial innovation, but is also associated with a number of risks. These include security risk and risks associated with a lack of regulation. The regulatory status of market infrastructures for decentralised finance are somewhat unclear under the Markets in Crypto-Assets Regulation proposed by the European Commission. Even if such market infrastructures were to come under the regulation, it is unclear how the regulation would be enforced if such market infrastructures were operated in a decentralised manner. Decentralised finance will amplify some of the challenges associated with market infrastructures for trading in tokenised assets as mentioned above. It will be less possible to correct automated smart contracts in the event of errors, and it will be even more difficult to enforce court decisions and implement other public interventions that interpose themselves in contracts.

Norges Bank is monitoring developments in market infrastructures for trading in tokenised assets, including decentralised finance. If a substantial portion of trade is transferred to market infrastructures for trading in tokenised assets, they may come to play a systemic role with implications for financial stability.

These developments are also relevant for research into CBDCs. It is possible that a CBDC, if introduced, should be designed to realise the gains from programmable money and market infrastructures for trading in tokenised assets. In that case, it should be in a manner providing an acceptable risk, which requires, among other things, the establishment of a regulatory framework. CBDCs are discussed further in Section 1.2, 1.2 Central bank digital currencies.

33 BIS (2020).
34 Allen et al (2020b).

RISKS ASSOCIATED WITH MARKET INFRASTRUCTURES FOR TOKENISED ASSETS AND THE USE OF SMART CONTRACTS

Smart contracts are neither smart nor contracts in the legal sense. Owing to programming errors, automated transactions may be executed in a manner different from the one agreed by the parties. Automation can be a barrier to the execution of the contract as intended. In certain cases, the only alternative may be to execute the automated contract and establish a new automated contract that corrects the one executed. This increases transaction costs and raises new issues if, for example, one of the parties is not agreeable or goes bankrupt.

Programming errors can also entail vulnerabilities that third parties can use to acquire assets or confidential information that can be exploited for financial gain. This raises new issues relating to liability and the possibility of reversing transactions.

Furthermore, it is impossible in practice to regulate in advance all eventualities that may arise in a contractual relationship. Potential disputes over valuation can hardly be resolved with program code alone, eg what is a "warranted expectation" or what is "reasonable". If a smart contract is entered into by a person not legally entitled or authorised to do so, the validity of the contract may be null and void. If a legal dispute arises and ends with a court decision, it needs to be practicable for the parties to enforce the decision. In traditional contractual relationships, this may be ultimately settled by an enforcement order. This might typically entail that a bank is ordered to withdraw amounts from a debtor's account or a central securities depository or other securities register is ordered to change the register entry in accordance with the court order. If the parties have used a tokenised form of money, such as stablecoins, such enforcement may be more difficult and other instrumentalities may be necessary to enforce a court order.

There is research internationally on how effective dispute resolution systems can be implemented for smart contracts on infrastructures for trading in tokenised assets.[1] This involves both how dispute resolution systems can be implemented as an integral part of such infrastructure and integration with external legal decisions and regulatory interventions.

The cryptographic platforms that are used to ensure that crypto-asset systems and infrastructures for trading in tokenised assets are more closely tied to the infrastructure than is the case for traditional platforms. Cryptography is not only a module for secure communication, but the actual ownership of assets is linked to a cryptographic architecture and control over cryptographic codes. This creates at least two types of risk. First, owing to the strong connection between control over cryptographic codes and ownership, these systems may be particularly exposed to vulnerabilities in the cryptographic platforms, in that it may be more difficult to distinguish between rightful owners and attackers. Second, the integration of cryptographic platforms with ownership may increase the difficulty of smooth and agile replacement of cryptographic infrastructure if necessary. For example, it may be necessary for users to take active steps to move the assets onto new and more secure platforms. If the development of these systems is decentralised, additional coordination will be necessary to meet challenges related to vulnerabilities in cryptographic platforms and in the event of other needs to replace platforms.–

1 WEF (2020).

References

Allen, S., Capkun, S., Eyal, I., Fanti, G., Ford, B., Grimmelmann, J. and Prasad, E. (2020a), "Design Choices for Central Bank Digital Currency: Policy and Technical Considerations". Brookings working paper. https://www.brookings.edu/research/design-choices-for-central-bank-digital-currency-policy-and-technical-considerations/

Allen, J. G., Rauchs, M., Blandin, A., and Bear, K. (2020b), *Legal and Regulatory Considerations for Digital Assets*. https://www.jbs.cam.ac.uk/wp-content/uploads/2020/10/2020-ccaf-legal-regulatory-considerations-report.pdf

BIS (2020), Project Helvetia: Settling tokenised assets in central bank money. https://www.bis.org/publ/othp35.htm

BIS (2021a), "Covid-19 and cyber risk in the financial sector", BIS Bulletin No 37, 14 January 2021. https://www.bis.org/publ/bisbull37.pdf

BIS (2021b), "Supervising cryptoassets for anti-money laundering", FSI Insights No 31. https://www.bis.org/fsi/publ/insights31.htm

Boar, C. and A. Wehrli (2021), "Ready, steady, go? – Results of the third BIS survey on central bank digital currency". BIS Papers No. 114. https://www.bis.org/publ/bppdf/bispap114.pdf

CPMI-IOSCO (2012), *Principles for Financial Market Infrastructures*. https://www.bis.org/cpmi/publ/d101a.pdf

Danmarks Nationalbank (2018), *TIBER-DK General Implementation Guide*, 18 December 2018. https://www.nationalbanken.dk/da/publikationer/Documents/2018/12/NYT_nr%207_Test%20skal%20oege%20cyberrobustheden%20i%20Danmark.pdf#search=tiber

ECB (2018), *TIBER-EU Framework, How to implement the European framework for Threat Intelligence-based Ethical Red Teaming*, May 2018. https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf

ESRB (2020), *Systemic cyber risk*. https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf

European Commission (2019), *Digital Operational Resilience Framework for financial services: Making the EU financial sector more secure*. https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/2019-financial-services-digital-resilience-consultation-document_en.pdf

European Commission (2020a), "Digital finance package". https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en

European Commission (2020b), Proposal for a regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, COM/2020/593 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX-:52020PC0593

European Commission (2020c), Proposal for a regulation of regulation of the European Parliament and of the Council on a pilot regime for market infrastructures based on distributed ledger technology. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0594

European Commission (2020d), Digital Single Markets, Online Platforms. https://ec.europa.eu/digital-single-market/en/online-platforms

FSB (2020), *Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements*. https://www.fsb.org/2020/10/regulation-supervision-and-oversight-of-global-stablecoin-arrangements/

IMF Staff Country Report: Norway (2020),: Financial Sector Assessment Program-Technical Note-Cybersecurity Risk Supervision and Oversight. https://www.imf.org/en/Publications/CR/Issues/2020/08/07/Norway-Financial-Sector-Assessment-Program-Technical-Note-Cybersecurity-Risk-Supervision-and-49673

Karantias, K. (2020), "SoK: A Taxonomy of Cryptocurrency Wallets". IACR Cryptology ePrint Archive, 2020: 868. https://eprint.iacr.org/2020/868.pdf

Norges Bank (2014), *Financial Infrastructure Report* 2014. https://www.norges-bank.no/en/news-events/news-publications/Reports/Financial-Infrastructure-Report/Financial-infrastructure-report-2014/

Norges Bank (2019), *Financial Infrastructure Report* 2019. https://www.norges-bank.no/en/news-events/news-publications/Reports/Financial-Infrastructure-Report/financial-infrastructure-2019/

Norge Bank (2020a), *Norway's financial system* 2020. https://www.norges-bank.no/en/news-events/news-publications/Reports/norways-financial-system/2020-dnfs/

Norges Bank (2020b), *Financial Infrastructure Report* 2020. https://www.norges-bank.no/en/news-events/news-publications/Reports/Financial-Infrastructure-Report/finansiell-infrastruktur-2020/

Norges Bank (2020c), "Norges Banks vurdering av interbanksystemet NICS, og DNBs og SpareBank 1 SMNs oppgjørsbanksystem mot internasjonale prinsipper for finansielle infrastrukturer" [Norges Bank's assessment of the interbank system NICS and DNB's and SpareBank 1 SMN's settlement systems against international principles for financial market infrastructures]. *Norges Bank Papers* 4/2020 (Norwegian only). https://www.norges-bank.no/aktuelt/nyheter-og-hendelser/Publikasjoner/Norges-Bank-Memo-/2020/memo-42020/

Norges Bank (2020d), *Norges Banks oppgjørssystem, Egenvurdering mot internasjonale prinsipper for finansiell infrastruktur* [Norges Bank's settlement system. Self-assessment against international principles for financial market infrastructures] (Norwegian only). https://www.norges-bank.no/contentassets/6e6ca7f8e69a4b259342944ad3284133/pfmi-egenvurdering-nbo-2019.pdf?v=05/25/2020134350&ft=.pd&v=05/25/2020134350&ft=.pd

Norges Bank (2021), "Central Bank Digital Currencies" *Norges Bank Papers* 1/2021.

Norwegian Government (2021), "Bankenes tilbud av kontanttjenester – høringsnotat" [Banks' provision of cash services – Consultation document] (Norwegian only). https://www.regjeringen.no/contentassets/66471a4f52354513b86d082433dfcee2/brev_2021-04-23-ft-kontanter.pdf

Norwegian National Security Authority (2020), Alert from NSM/NCSC, 22 December 2020. New back door in SolarWinds Orion (Norwegian only). https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/varsler-fra-ncsc/ny-bakdor-i-solarwinds-orion

Norwegian Police Security Service (2020), Nasjonal trusselvurdering [National threat assessment] (Norwegian only). https://pst.no/alle-artikler/trusselvurderinger/nasjonal-trusselvurdering-2020/

Østbye, P. (2020), "Hva er desentralisert finans, og bør sentralbanker bry seg?" [What is decentralised finance, and should central banks care?] Blog post on the *Bankplassen* blog (Norwegian only). https://bankplassen.norges-bank.no/2020/11/19/hva-er-desentralisert-finans-og-bor-sentralbanker-bry-seg/

Sai, A. R., Buckley, J., Fitzgerald, B., and Gear, A. L. (2020), "Taxonomy of Centralization in Public Blockchain Systems: A Systematic Literature Review". *arXiv preprint arXiv:2009.12542*. https://arxiv.org/abs/2009.12542

WEF (2020), "Bridging the Governance Gap: Dispute resolution for blockchain-based transactions", White paper, December 2020. http://www3.weforum.org/docs/WEF_WP_Dispute_Resolution_for_Blockchain_2020.pdf

Annex[1]

Table 1: Average daily turnover in clearing and settlement systems (transactions)

	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
NICS											
NICS Gross	568	548	594	659	624	772	980	1 021	1 567	1 859.0	2 027.9
NICS Net (million)	6.8	7.2	7.8	8.2	8.7	9.1	9.5	9.9	10.5	11.1	10.1
NICS Real											333 255[1]
NBO											
Total number of transactions	1 146	1 138	1 274	1 406	1 367	1 565	1 835	1 958	2 555	2 745	2 935
RTGS Gross transactions excl. NICS	477	479	549	595	592	658	700	793	841	859	930

1 The daily average for NICS Real is calculated using the number of calendar days from April 2020.

Sources: The figures under NICS are from Bits. The figures under NBO are from Norges Bank

Table 2: Average daily turnover in clearing and settlement systems (in billions of NOK)

	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
NICS	**196.5**	**221.4**	**247.8**	**253.5**	**262.8**	**285.9**	**284.1**	**297.0**	**315.3**	**323.2**	**346.7**
NICS Gross	107.2	119.1	138.6	136.0	140.9	160.1	158.7	163.3	175.2	176.0	196.1
NICS Net	89.3	102.3	109.2	117.5	121.9	125.8	125.4	133.7	140.1	147.2	150.6
NICS Real											0.2[1]
NBO	**162.2**	**172.1**	**201.9**	**188.3**	**198.0**	**219.3**	**221.2**	**235.8**	**247.6**	**259.3**	**458.1**
NICS Gross	106.3	119.0	137.7	135.2	140.8	157.5	156.1	159.0	172.2	158.0	178.5
RTGS Gross transactions excl. NICS	42.5	42.4	51.1	38.5	42.5	46.0	40.4	42.1	57.3	81.7	261.5
NICS Net	7.1	6.3	8.7	10.3	10.8	11.9	12.4	13.1	13.3	13.5	13.4
NICS Real											0.0
VPO and Oslo Clearing[2]	5.3	4.5	4.4	4.2	3.9	3.8	3.7	4.2	4.8	6.0	4.7
VPO	5.2	4.5	4.4	4.2	3.9	3.8	3.6	4.2	4.8	6.0	5.4
Oslo Clearing	0.1	0.1	0.0	0.0	0.1	0.0	0.0	0.0	0.0	0.0	0.0

1 The daily average for NICS Real is calculated using the number of calendar days from April 2020.
2 Legally integrated with SIX x-clear from May 2015.

Sources: The figures under NICS are from Bits. The figures under NBO are from Norges Bank

1 For tables showing developments in retail payment services, see *Norges Bank Papers* 2/2021.

Tabell 3: Number of participants in clearing and settlement systems (at year-end)

	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Norges Bank's settlement system (NBO): Banks with account in Norges Bank	**134**	**129**	**131**	**128**	**131**	**129**	**129**	**124**	**127**	**129**	**122**
Norges Bank's settlement system (NBO): Banks with retail net settlement in Norges Bank	21	21	22	22	21	22	22	21	21	21	21
DNB	105	103	98	98	97	94	94	93	92	90	87
SpareBank 1 Midt-Norge	13	12	11	11	11	11	11	11	10	10	10
Norwegian Interbank Clearing System (NICS)	142	138	132	131	130	128	128	125	124	122	119

Source: Norges Bank

NORGES BANK
Bankplassen 2, P.O. Box 1179 Sentrum, N-0107 Oslo
www.norges-bank.no

Financial Infrastructure Report 2021